UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/580,689	05/30/2000	Arturo Maria	83531-231	1763

22504 .7590 01/22/2008

DAVIS WRIGHT TREMAINE, LLP/Seattle
1201 Third Avenue, Suite 2200
SEATTLE, WA 98101-3045

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
01/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/580,689	MARIA, ARTURO	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-14,23-30 and 32-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-14,23-30 and 32-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/29/2007 has been entered.

Response to Arguments

2. In response to communications filed on 10/29/2007, the following claims 1-5, 7-14, 23-30, and 32-43 are pending and are presented for examination.

2.1 Applicant's arguments, pages 8-11, filed on 10/29/2007, with respect to the rejection of claims 1-5, 7-14, 23-30, and 32-43 have been fully considered but they are not persuasive. In response to Applicant's arguments that Yavatkar teaches away from combining with Lavian, the section cited by Applicant (Yavatkar, column 4, lines 30-35) is not sufficient for making such allegation because this passage merely describes that it may be wise to use the mobile agent alone in a specific case where "network attacks may start and stop quickly

"Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. *In re Susi*, 440 F.2d 442, 169 USPQ 423 (CCPA 1971).... Furthermore, "[t]he prior art's mere

disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed..." *In re Fulton*, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004)." (See MPEP § 2123).

Applicant argues on page 9 that Lavian does not mention anything about attack or countering intrusions to a network. Examiner respectfully disagrees because Lavian discloses monitoring whether network traffic is beyond a particular threshold and performing action in response which is interpreted by Examiner as a network intrusion detection/response. Applicant's specification refers to and not limited to increase or decrease of network traffic as examples intrusion detection (see for instance page 5, lines 1-5 and lines 25-27). Therefore, Examiner's interpretation of intrusion detection is proper. In addition, the motivation statement does not have to be cited word for word in the reference as explained in the last office action on page 2 as network attack due to increase of network traffic beyond a particular threshold is within the knowledge generally available to one of ordinary skill in the art. In response to applicant's arguments regarding Sprunk, Examiner asserts that prevention of viruses and hackers in a network system is not significantly different from network intrusion and the prevention is not simply within a PC as Brown discloses the PC is connected to an Internet service provider. In response to applicant's argument that Brown is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, in response to applicant's arguments that Brown is

unrelated to any intrusion detection technology, Brown has been used for disclosing the particular problem that applicant is concerned which is changing the number of computers for executing software depending on time of day.

Therefore as indicated above, applicant has not overcome the rejection in view of the prior art. Examiner does not concede to any of applicant's arguments as explained above. Upon further consideration and to expedite the prosecution, a new ground of rejection is set forth below in view of the previously cited prior art and Jansen (newly cited).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 7-10, 14, 23, 27-30, and 32-35 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,842,781 to **Lavian et al**.

As per claim 1, Lavian et al discloses a method for implementing an intrusion detection system in a network, comprising: receiving request from the NMS server at a software agent

installed on each of a plurality of network devices to load a set of operations associated with a particular task on each respective one of the one or more network devices (plurality of computers) (see column 7, lines 43-45 and column 3, lines 23-27) that meets the recitation of *receiving a request from a central server at a software agent program installed on each respective one of the plurality of computers to initiate intrusion detection services on each respective one of the plurality of remote computers* wherein the request is issued by the central server in response to a notification of inactivity on the network or the network traffic increases beyond a particular threshold (see column 3, lines 35-40 and column 8, lines 2-6) that meets the recitation of *wherein the request is issued in response to a notification of a network intrusion*; and discloses installing and executing the software on the one or more computers (via a software agent residing at each device col. 9, lines 44-46) in response to the request (see column 7, lines 50-67 and column 3, lines 22-27 and lines 47-50) that meets the recitation of *installing intrusion detection software on said remote computer via said software agent program*, and *executing said intrusion detection software on said remote computer via said software agent program.*

As per claim 7, Lavian et al discloses determining if a network device should or should not receive a particular application (see column 3, lines 11-18) that meets the recitation of selecting said remote computers from a plurality of eligible computers.

As per claim 8, Lavian et al discloses a network table including a list of network addresses associated with network devices to assist in requests from the network management

application (see column 6, lines 16-27) that meets the recitation of said selecting step is accomplished based on a network map.

As per claim 9, Lavian et al discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (see column 6, lines 16-27 and column 3, lines 8-21 and 47-50).

As per claims 10 and 14, Lavian et al discloses wherein said request is verified using a cryptographic authentication scheme (see column 3, lines 8-21).

As per claim 23, Lavian et al discloses a system for detecting intrusions in a computer network comprising: receiving request from the NMS server (*intrusion detection server*) at a software agent installed on each of a plurality of network devices to load a set of operations associated with a particular task on each respective one of the one or more network devices (*a plurality of computers executing software agents*) (see column 7, lines 43-45 and column 3, lines 23-27) and also discloses a database to facilitate converting object oriented requests for MIB information into requests for network parameters (see column 5, lines 35-53); and a network table including a list of network addresses associated with network devices to assist in requests from the network management application (see column 6, lines 16-27) wherein the request is issued by the central server in response to a notification of inactivity on the network or the network traffic increases beyond a particular threshold (see column 3, lines 35-40 and column 8, lines 2-6 and column 10, lines 44-50) to perform installing and executing the software on the one

or more computers (via a software agent residing at each device col. 9, lines 44-46) in response to the request (see column 7, lines 50-67 and column 3, lines 22-27 and lines 47-50) that meets the recitation of *a database configured to store at least one rule defining at least one response to a network intrusion, wherein said intrusion detection server is configured to send a request to install and execute intrusion detection software to software agents at the plurality of computers when intrusion detection services are needed based on the at least one rule stored in said database.*

As per claim 27, Lavian et al discloses the limitation of wherein said database contains information about the plurality of computers (see column 6, lines 16-27).

As per claim 28, Lavian et al discloses a network table including a list of network addresses associated with network devices to assist in requests from the network management application (see column 6, lines 16-27) that meets the recitation of wherein said information includes a map of said computer network.

As per claim 29, Lavian et al discloses the limitation of wherein said database contains a knowledge base (see column 6, lines 16-27 and column 3, lines 8-21 and 47-50).

As per claim 30, Lavian et al discloses a n article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which when executed defined a series of steps comprising: *receiving*

notification of a network intrusion at a central server (see column 3, lines 35-40 and column 8, lines 2-6); receiving request from the NMS server at a software agent installed on each of a plurality of network devices to load a set of operations associated with a particular task on each respective one of the one or more network devices (plurality of computers) (see column 7, lines 43-45 and column 3, lines 23-27) wherein the request is issued by the central server in response to a notification of inactivity on the network or the network traffic increases beyond a particular threshold (see column 3, lines 35-40 and column 8, lines 2-6) that meets the recitation of *transmitting an intrusion detection software installation request from the central server to a plurality of remote computers at a software agent program installed on each respective one of the plurality of computers to initiate intrusion detection services on each respective one of the plurality of remote computers in response to the notification* and discloses installing and executing the software on the one or more computers (via a software agent residing at each device col. 9, lines 44-46) in response to the request (see column 7, lines 50-67 and column 3, lines 22-27 and lines 47-50) that meets the recitation of *installing intrusion detection software on the plurality of remote computers via said software agent program in response to the request.*

As per claim 32, Lavian et al discloses determining if a network device should or should not receive a particular application (see column 3, lines 11-18) that meets the recitation of selecting said remote computers from a plurality of eligible computers.

As per claim 33, Lavian et al discloses a network table including a list of network addresses associated with network devices to assist in requests from the network management

application (see column 6, lines 16-27) that meets the recitation of said selecting step is accomplished based on a network map.

As per claim 34, Lavian et al discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (see column 6, lines 16-27 and column 3, lines 8-21 and 47-50).

As per claim 35, Lavian et al discloses wherein said request is verified using a cryptographic authentication scheme (see column 3, lines 8-21).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-4, 11, 13, 24-26, 36, 38 and are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,842,781 to **Lavian et al** in view of Non-Patent Literature "Applying Mobile Agents to Intrusion Detection Response" Pages 1-46 by **Jansen et al.**

As per claim 2, Lavian et al does not explicitly disclose terminating intrusion detection services. **Jansen et al** in an analogous art teaches Intrusion Detection system and further discloses as traffic characteristic changes mobile agents should adapt dynamically, for instance a mobile agent may be requested to be terminated as network and host conditions change (see section 3.1.5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Lavian et al** to issue a request to terminate intrusion detection services at said software agent program so as to adapt to changes and host conditions as suggested by **Jansen et al.**

As per claim 3 the combination of references above discloses the limitation of monitoring for fulfillment of a stop condition (see **Jansen et al**, section 3.1.5). This claim is also rejected on the same rationale as the rejection of claim 2 above.

As per claims 4 and 13, the combination of references above discloses wherein said stop condition is based on network traffic conditions (see **Jansen et al**, section 3.1.5*)*. This claim is also rejected on the same rationale as the rejection of claim 2 above.

As per claim 11, the combination of references above discloses wherein said request includes a stop condition indicating when to stop executing the intrusion detection software (see **Jansen et al**, section 3.1.5). This claim is also rejected on the same rationale as the rejection of claim 2 above.

As per claim 24, the combination of references above discloses wherein said intrusion detection server increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected (see **Jansen et al**, sections 3.1.1 and 3.1.5). This claim is also rejected on the same rationale as the rejection of claim 2 above.

As per claim 25, the combination of references discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes (see **Jansen et al**, sections 3.1.1, 3.1.2, and 3.1.5).

As per claim 26, the combination of references discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software in real time. **Jansen et al** further discloses that the dispatched agents are adapted dynamically in real time depending how the traffic characteristics change over time (see section 3.1.5) one of ordinary skill in the art understands that network traffic varies according to time of day that meets the recitation of wherein said intrusion detection server changes the

number of said plurality of computers executing intrusion detection software depending on the time of day.

As per claim 36, the combination of references above discloses wherein said request includes a stop condition indicating when to stop executing the intrusion detection software (see **Jansen et al**, section 3.1.5). This claim is also rejected on the same rationale as the rejection of claim 2 above.

As per claim 38, the combination of references above discloses wherein said stop condition is based on network traffic conditions (see **Jansen et al**, section 3.1.5*)*. This claim is also rejected on the same rationale as the rejection of claim 2 above.

4. **Claims 5, 12, 37, and 41-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,842,781 to **Lavian et al** in view of Non-Patent Literature "Applying Mobile Agents to Intrusion Detection Response" Pages 1-46 by **Jansen et al** as applied to claims 2-4 and further in view of US Patent Publication 2002/0003884 to **Sprunk.**

As per claims 5, 12, and 37, neither of the references explicitly discloses that the stop condition is an expiration time. **Sprunk** in an analogous art teaches a secure access system comprising an access control processor (ACP) for monitoring which application objects are executed in a computer system and to confirm their authorization and authenticity. Although the exemplary embodiment uses set top boxes, the invention is applicable to PC computers, which

are susceptible to viruses, and hackers as disclosed in the background. **Sprunk** discloses that checkpoints are embedded in the applications on each system to trigger the ACP, and among the features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) and further discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of wherein the stop condition is an expiration time. As interpreted by the Examiner, the execution of the software will stop on all computers with a date/time expiration status. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk**. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

As per claim 41, neither of the references explicitly state that the stop condition applies to all eligible computers. **Sprunk** in an analogous art teaches a secure access system comprising an access control processor (ACP) for monitoring which application objects are executed in computer systems and to confirm their authorization and authenticity. Although the exemplary embodiment uses set top boxes, the invention is applicable to PC computers, which are susceptible to viruses, and hackers as disclosed in the background. **Sprunk** discloses that

checkpoints are embedded in the applications on each system to trigger the ACP, and among the features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) and further discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of a stop condition indicating when to stop executing the intrusion detection software program and wherein the stop condition applies to all eligible computers. As interpreted by the Examiner, the execution of the software will stop on all computers with a date/time expiration status. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped in the event that an unauthorized object is detected as suggested by **Sprunk**. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on what applications or objects are authorized to be executed on each computer system.

As per claim 42, Sprunk discloses a monitoring process wherein checkpoints are embedded in the applications on each system to trigger the ACP, and among the features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) that meets the recitation of monitoring for fulfillment of a stop condition at each of the plurality of remote computers executing intrusion detection software (see paragraphs 5, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped at each of the plurality of remote computers because it would allow the software to stop execution in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk** above. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

As per claim 43, Sprunk discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of wherein the stop condition for each of the plurality of computers is based on a time during which each of the plurality of remote computers has been executing intrusion detection software (see paragraphs 5, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped at each of the plurality of remote computers when executing intrusion detection software because it would allow the software to stop execution in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk** above. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

5. **Claims 39-40** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,842,781 to **Lavian et al** in view of US Patent 6,401,238 to **Brown et al.**

As per claim 39, Lavian et al does not explicitly disclose applications are initiated at a plurality of remote computers selected based on a number of platforms that are currently active. **Brown et al** in an analogous art teaches intelligent deploy of application to given machines in a network by a server based on criteria to reflect user needs and network environment (see column 1, lines 40-45). **Brown et al** further discloses determining which of a given set of users (client machines) have a given priority based on a user profile wherein the monitored condition is based on time of day (see column 8, lines 10-11 and 29-30 and abstract) **Brown et al** discloses applications are initiated at a plurality of remote computers selected based on a number of platforms that are currently active as the server monitors current bandwidth utilization as a measure of traffic over a short period immediately preceding the call to the server that meets the recitation of wherein intrusion detection services axe initiated at a plurality of remote computers selected based on a number of platforms that are currently active (see column 5, lines 40-47 and column 6, lines 39-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to initiate intrusion detection services at a plurality of remote computers selected based on a number of platforms that are currently active as suggested by **Brown et al**. One of ordinary skill in the art would have recognized the advantage of providing an intelligent deployment of applications that controls the

use of network bandwidth and network priorities as suggested by **Brown et al** (see column 1, lines 26 through column 2, line 25).

As per claim 40, Brown et al discloses applications are initiated at a plurality of remote computers selected based on network usage to minimize congestion and predetermined rules that take into consideration high and low network usage (see column 6, lines 1-8 and 58-67 and column 1, lines 11-21 and fig. 4) that meets the recitation of wherein intrusion detection services axe initiated at a plurality of remote computers selected based on based on predetermined numbers of maximum and minimum limits on a number intrusion detection platforms (see column 5, lines 40-47 and column 6, lines 39-47). Therefore claim 40 is rejected on the same rationale as the rejection of claim 39 above.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/

Carl Colin
Patent Examiner, A.U. 2136
January 8, 2008